REPORTING

When reporting a computer crime involving state computer resources, please call the California State Warning Center at (916) 845-8931 and be prepared to provide the following information:

- Name and address of the reporting agency.
- Name, address, e-mail address, and phone number(s) of the reporting person.
- Name, address, e-mail address, and phone number(s) of the Information Security Officer (ISO).
- Name, address, e-mail address, and phone number(s) of the alternate contact (e.g., alternate ISO, system administrator, etc.)
- Description of the incident.
- Date and time the incident occurred.
- Date and time the incident was discovered.
- Make/model of the affected computer(s).
- IP address of the affected computer(s).
- Assigned name of the affected computer(s).
- Operating System of the affected computer(s).
- Location of the affected computer(s).

SEVEN SIMPLE COMPUTER SECURITY TIPS

- **Use strong passwords.** Choose passwords that are difficult or impossible to guess. Give different passwords to all accounts.
- **Make regular backups of critical data.** Backups must be made at least once each day. Larger organizations should perform a full backup weekly and incremental backups every day. At least once a month the backup media should be verified.
- **Use virus protection software.** That means three things: having it on your computer in the first place, checking daily for new virus signature updates, and then actually scanning all the files on your computer periodically.
- **Use a firewall as a gatekeeper between your computer and the Internet.** Firewalls are usually software products. They are essential for those who keep their computers online through broadband connections such as DSL or cable, but they are also valuable for those who still dial in.
- **Do not keep computers online when not in use.** Either shut them off or physically disconnect them from Internet connection.
- **Do not open e-mail attachments from strangers,** regardless of how enticing the Subject Line or attachment may be. **Be suspicious of any *unexpected* e-mail attachment from someone you *do* know** because it may have been sent without that person's knowledge from an infected machine.
- **Regularly download security patches from your software vendors.**

**Consult* www.sans.org/top20/ *for more info.*

CHP 1040 (rev. 4/3) OPI 040

California Highway Patrol

Computer Crime Reporting for State Agencies

LEGAL REQUIREMENTS

Government Code Section 14613.7(a) requires state agencies to report to the California Highway Patrol (CHP) all crimes on state-owned or state-leased property where state employees are discharging their duties. This includes the reporting of crimes involving state computer resources. *(Note: Notification of a computer crime to a local law enforcement agency or IT related investigative task force does not relieve state agencies of their obligation to notify the CHP.)*

The California State Warning Center is available 24 hours a day, seven days a week, to receive reports of computer crimes from state agencies.

We recommend that representatives of state agencies reporting computer crimes to the CHP follow their established internal departmental notification protocols, and to include involving the department's Information Security Officer, or his/her designee. State agencies reporting computer crimes to the California State Warning Center should be prepared to provide the information identified in the "**REPORTING**" section of this brochure. When the California State Warning Center receives a report of a computer crime, CHP Investigators are immediately notified.

Depending on the nature of the computer crime reported, a CHP Investigator may respond to, or call, the reporting agency for additional information.

COMPUTER CRIMES THAT REQUIRE IMMEDIATE NOTIFICATION TO THE CHP

The CHP has primary investigative authority for violations of California Penal Code Section 502, subsection (c), where a state agency is the victim. Computer crimes occur when a person:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network..

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.